GCCC Q&As

GCCC - GIAC Critical Controls Certification (GCCC)

Pass GIAC GCCC Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/gccc.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Of the options shown below, what is the first step in protecting network devices?

A. Creating standard secure configurations for all devices

B. Scanning the devices for known vulnerabilities

C. Implementing IDS to detect attacks

D. Applying all known security patches

Correct Answer: A

QUESTION 2

IDS alerts at Service Industries are received by email. A typical day process over 300 emails with fewer than 50 requiring action. A recent attack was successful and went unnoticed due to the number of generated alerts.

What should be done to prevent this from recurring?

A. Tune the IDS rules to decrease false positives.

B. Increase the number of staff responsible for processing IDS alerts.

C. Change the alert method from email to text message.

D. Configure the IDS alerts to only alert on high priority systems.

Correct Answer: A

QUESTION 3

An organization has implemented a control for Controlled Use of Administrative Privilege. The control requires users to enter a password from their own user account before being allowed elevated privileges, and that no client applications (e.g. web browsers, e-mail clients) can be run with elevated privileges. Which of the following actions will validate this control is implemented properly?

A. Check the log entries to match privilege use with access from authorized users.

B. Run a script at intervals to identify processes running with administrative privilege.

C. Force the root account to only be accessible from the system console.

Correct Answer: B

QUESTION 4

Which of the following best describes the CIS Controls?

A. Technical, administrative, and policy controls based on research provided by the SANS Institute

B. Technical controls designed to provide protection from the most damaging attacks based on current threat data

C. Technical controls designed to augment the NIST 800 series

D. Technical, administrative, and policy controls based on current regulations and security best practices

Correct Answer: B

QUESTION 5

When evaluating the Wireless Access Control CIS Control, which of the following systems needs to be tested?

A. Log management system

B. 802.1x authentication systems

C. Data classification and access baselines

D. PII data scanner

Correct Answer: B